

CEH version 10 Practice Test Questions (Answer Key)

Guards, lights, and cameras are examples of ____ security controls:

- A) Technical
- B) Administrative
- C) Physical**
- D) Additional

Explanation: These are examples of physical security controls. Technical controls include things like encryption, smart cards, and access control lists (ACLs). Administrative controls include employee training and awareness. Additional is a made up answer.

These are attacks on the actual programming code and software logic of an application.

- A) Misconfiguration attack
- B) Application level attack**
- C) Shrink wrap attack
- D) OS attack

Explanation: Application-level attacks are attacks on the actual programming itself (the code and software logic). A shrink-wrap attack takes advantage of built-in code and scripts that come with most off the shelf applications. OS attacks target operating system vulnerabilities and default installation behavior. Misconfiguration attacks take advantage of systems that are not properly configured for security.

This attack takes advantage of built-in code and scripts in off the shelf applications and other free libraries and code.

- A) Application level attack
- B) Shrink wrap attack**
- C) Misconfiguration attack
- D) Roger-wrap attack

Explanation: Shrink wrap (or shrink-wrap) is correct. Application-level attacks are attacks on the actual programming itself (the code and software logic). Misconfiguration attacks take advantage of systems that are not properly configured for security. Roger-wrap attack is a made up answer.

The four parts of Common Criteria (CC) are:

- A) BB, TOE, PP, SL
- B) EAL, TOE, ST, PP**
- C) EAL, TOE, TS, PP
- D) EAL, MAC, ST, PP

Explanation: The parts of Common Criteria are Evaluation Assurance Level (EAL), Target of Evaluation (TOE), Security Target (ST), and Protection Profile (PP).

In this type of test, the ethical hacker has no knowledge of the target.

- A) Grey box
- B) White box
- C) Black box**
- D) Blue box

Explanation: Black box testing is generally where the ethical hacker has no knowledge of the target, so it will simulate a “real attacker.” Grey box testing is a partial knowledge test to simulate more of an insider attack. White box testing is where full knowledge of the network is known (i.e.- the network infrastructure, critical business systems, etc...). Blue box is a made up answer.

This is used to identify systems and processes that are critical for operations.

- A) Black box test
- B) BIA**
- C) BCP
- D) DRP

Explanation: This is not mentioned in the official ECC book. The Business Impact Analysis (BIA) is correct. Business Continuity Plan (BCP) is a set of plans and procedures to follow in the event of a failure or disaster to main business operations, The Disaster Recovery Plan (DRP) addresses what to do to recover IT systems after a disaster has occurred. The Black box test is generally where the ethical hacker has no knowledge of the target, so it will simulate a “real attacker” and does not apply.

A health care law.

- A) SOX
- B) HIPPA
- C) HIPAA**
- D) PCI

Explanation: HIPAA is a health care law that covers protecting protected health information (PHI). Sarbanes-Oxley (SOX) is designed to protect investors from shady financial reporting by companies. PCI-DSS (Payment Card Industry Data Security Standard) covers organizations that handle credit/debit card processing. HIPPA is made up and, unfortunately, is how many health care professionals reference the HIPAA law.

According to EC-Council, footprinting is the ____ step of an attack on information systems.

- A) Last
- B) First**
- C) third
- D) fourth

Explanation: Footprinting is the first step of an attack on information systems.

This law makes conspiracy to commit hacking a crime.

- A) SOX
- B) HIPAA
- C) Computer Fraud and Abuse Act**
- D) Hacking Fraud Act

Explanation: HIPAA covers protecting PHI for health care organizations. SOX is to protect investors from shady financial reporting. Hacking Fraud Act is made up.

In Google hacking, filetype:XLS

- A) displays pages with directory browsing enabled
- B) searches for only files of a specific type**
- C) displays pages with a string in the URL
- D) displays linked pages based on a search term

Explanation: This (filetype) particular Google hacking command is not mentioned in the official EC-Council material. The index command displays pages with directory browsing enabled. The inurl command displays pages with a string in the URL. The link command displays linked pages based on a search term.

The inurl command.

- A) restricts results to only the pages that contain the word or string specified in the URL**
- B) opens a new browser window with the URL
- C) displays linked pages based on a search term
- D) searches for file of a specific type

Explanation: The link command displays linked pages based on a search term. The filetype command searches for file of a specific type. The answer of opening a new browser window with the URL is a made up answer.

The intitle command:

- A) display linked pages based on a search term
- B) restricts results to only the pages containing the specified term in the title**
- C) restricts results to only the pages that contain the word or string specified in the URL
- D) searches for only files of a specific type

Explanation: The link command displays linked pages based on a search term. The filetype command searches for file of a specific type. The inurl command restricts results to only the pages that contain the word or string specified in the URL.

This covers establishing, implementing, maintaining, and continually improving an information security plan.

- A) HIPAA
- B) ISO 27001:2013**
- C) ISO 2111:2019
- D) SOX

Explanation: HIPAA covers protecting PHI for health care organizations. SOX is to protect investors from shady financial reporting by companies. ISO 2111:2019 is a made up answer.

This tool can be used for Website mirroring.

- A) Wireshark
- B) HTTrack**
- C) SOA
- D) MX

Explanation: HTTrack is the only Website mirroring tool on the list and downloads a website from the Internet to a local directory. Wireshark is a network tool that allows you to capture traffic on a network. The Start of Authority (SOA) is a DNS record that is used to identify the primary name server for the zone. The MX (Mail Exchange) is also part of DNS records and identifies the e-mail servers within the domain.

This is a Windows command line tool that can be used to assign, display, or modify access control lists.

- A) cacls.exe**
- B) assign.exe
- C) adjust.exe
- D) aclss.exe

Explanation: This is not mentioned in the official ECC material. The command is cacls.exe and all of the other answers listed are made up.

This defines the hostname and port number of servers providing specific services, such as a Directory Services server.

- A) SOA
- B) MX
- C) SRV**
- D) CNAME

Explanation: SRV (Service) is correct. SOA (Start of Authority) identifies the primary name server for the zone. MX (Mail Exchange) identifies the e-mail servers within the domain. CNAME (Canonical Name) provides domain name aliases within your zone.

This identifies the primary name server for the zone and contains the hostname of the server responsible for all DNS records within a namespace.

- A) PTR
- B) SOA**

- C) CNAME
- D) NS

Explanation: The SOA (Start of Authority) identifies the primary name server for the zone. The CNAME (Canonical Name) provides domain name aliases within your zone. The Pointer (PTR) maps an IP address to a hostname. The Name Server (NS) defines the name servers within your namespace.

This identifies e-mail servers within the domain.

- A) NS
- B) CNAME
- C) MX**
- D) SOA

Explanation: MX (Mail Exchange) identifies the e-mail servers within the domain. The Name Server (NS) defines the name servers within your namespace. The CNAME (Canonical Name) provides domain name aliases within your zone. The SOA (Start of Authority) identifies the primary name server for the zone.

A (Address) does this.

- A) maps an IP address to a hostname and is used most often for DNS lookups.**
- B) identifies the e-mail servers within the domain.
- C) defines the name servers within your namespace.
- D) identifies the primary name server for the zone

Explanation MX (Mail Exchange) identifies the e-mail servers within the domain. The Name Server (NS) defines the name servers within your namespace. The SOA (Start of Authority) identifies the primary name server for the zone.

This record contains the source host, contact e-mail, serial number, refresh time, retry time, expire time, and TTL (time to live).

- A) SOA**
- B) MX
- C) CNAME
- D) PTR

Explanation: MX (Mail Exchange) identifies the e-mail servers within the domain. The CNAME (Canonical Name) provides domain name aliases within your zone. The Pointer (PTR) maps an IP address to a hostname.

All of the following are Website mirroring tools, EXCEPT:

- A) MmmmBop 3000**
- B) Black Widow
- C) WebRipper
- D) HTTrack

Explanation: Black Widow (Blackwidow in the ECC text), WebRipper, and HTTrack are all Website mirroring tools. MmmmBop 3000 is a made up answer. There was a song from the 1990's called something like Mmmmbop by a group named Hanson that happened to be stuck in my head, while I was creating this question, hence the MmmmBop 3000 tool was born.

This is the part of the SOA (Start of Authority) record that is the revision number of the zone file that increments each time a zone file changes. It is used by a secondary server to know when to update its copy.

- A) MX
- B) Serial Number**
- C) Name Server (NS)
- D) PTR

Explanation: MX (Mail Exchange) identifies the e-mail servers within the domain. The Name Server (NS) defines the name servers within your namespace. The Pointer (PTR) maps an IP address to a hostname.

A tool you can use for DNS queries is:

- A) Blackwidow
- B) Black Widow
- C) WebRipper
- D) DIG**

Explanation: DIG is a tool used for DNS queries. The other tools listed are for Website mirroring. Blackwidow and Black Widow are the same thing and are just listed differently in the AiO book versus the ECC text.

The hacker in the hoodie used nslookup to get a copy of a zone transfer. In the below output, what is 2013090800?

Listing domain [madeup.com]

Server: dn1234.madeup.com

Host or domain name	Resource	Record Info.
madeup.com	SOA	dn1234.madeup.com
hostmaster.madeup.com	(2013090800	86400 900 1209600 3600)

madeup.com	NS	DN1234.madeup.com
madeup.com	NS	DN5678.madeup.com
madeup.com	A	172.16.55.12
madeup.com	MX	30 mailsrv.madeup.com
mailsrv	A	172.16.101.5
www	CNAME	madeup.com
fprtone	A	172.16.101.15
fprttwo	A	172.16.101.16

- A) refresh interval
- B) serial number**
- C) TTL
- D) retry time

Explanation: The refresh interval is 86400. The TTL (time to live) is 3600. The retry time is 900. 1209600 is also the expiry time (not one of the answers).

All of the following are Internet registries EXCEPT:

- A) ARIN
- B) APNIC
- C) RIPE
- D) DIG**

Explanation: DIG is a tool used for DNS queries and is not an Internet registry. ARIN is the American Registry for Internet Numbers. APNIC is the Asia-Pacific Network Information Center. RIPE is Reseaux IP Europeens.

The OSI model includes all of the following layers EXCEPT:

- A) Transport
- B) Internet**
- C) Application
- D) Data Link

Explanation: The Internet layer is part of the TCP/IP model (Application, Transport, Internet, and Network Access layers) and not the OSI model (Physical, Data Link, Network, Transport, Session, Presentation, and Application layers).

The three-way handshake includes (choose the correct order):

- A) SYN, SYN/ACK, END
- B) ACK, SYN, SYN/ACK
- C) SYN, SYN/ACK, ACK**
- D) SRT, SYN/ACK, ACK

Explanation: SYN, SYN/ACK, ACK is the correct answer. The ACK, SYN, SYN/ACK answer does contain the correct items, just in the wrong order. The other two answers contain made up items (END and SRT).

An attacker gains access to a computer on the network, then uses the information gained to obtain access to other computers on the network.

A) daisy chaining

B) doxing

C) boxing

D) zero day

Explanation: Daisy chaining is correct. Doxing is when someone obtains your personally identifiable information (i.e.- your phone and address) and publishes it online. Boxing is a sport. Zero day is an attack that exploits a vulnerability before a patch is released/applied.

The formula for calculating the annualized loss expectancy (ALE) is:

A) $HKC + LEO = ALE$

B) $ALE = SLE \times ARO$

C) $ALE = SRT + REO$

D) $ABH = ALE \times GTO$

Explanation: The formula is $ALE \text{ (annualized loss expectancy)} = SLE \text{ (single loss expectancy)} \times ARO \text{ (annual rate of occurrence)}$. For your exam, just know what the letters stand for.

In the domain of cyber security, CIA stands for (choose the BEST answer):

A) Central Intelligence Agency

B) confidentiality, integrity, and availability

C) that movie with Dwayne "The Rock" Johnson

D) confidence, intelligence, and acumen

Explanation: The correct answer is confidentiality, integrity, and availability. The other answers are made up in regard to the topic of cyber security.

I use hacking tools developed by others, but I have no clue what I am really doing at a technical level. I am a:

A) Black Hat

B) White Hat

C) Script Kiddie

D) Big Bird

Explanation: The answer is script kiddie. Black and White Hat hackers know what they are doing at a technical level (at least we assume so). Big Bird is nothing nefarious (depending on your perspective) and is the bird on Sesame Street.

As an Ethical Hacker, I should start my pentest (choose the BEST answer):

- A) before I have a written agreement in place
- B) after I have a written agreement in place from the system owner that outlines exactly what is to be tested and what is off limits to eliminate any “gray” areas**
- C) at the convenience of the customer
- D) at the direction of my boss

Explanation: Always get permission first and make sure it is in writing to avoid visits from friendly people in nice suits.

I am a new hacker and want to see what old versions of a popular website looked like. I can go to (visit these sites at your own risk):

- A) www.dudewheresmycare.com
- B) www.archive.org**
- C) www.youtube.com
- D) www.funnycatvideos.com

Explanation: www.archive.org allows you to see copies of old websites, like Amazon. It's kind of neat to reminisce.

In this, name lookups generally use UDP and zone transfers generally use TCP.

- A) DNS**
- B) DIG
- C) ECC
- D) FTX

Explanation: DIG is a tool used for DNS queries. ECC stands for EC-Council. FTX stands for field training exercise (from the military).

This can help secure some DNS information.

- A) ECCCEH
- B) DNSSEC**
- C) DNS Runtime
- D) DNS PSN

Explanation: For the exam, just know DNSSEC is used to secure DNS information. ECCCEH stands for EC-Council Certified Ethical Hacker. DNS Runtime and DNS PSN are made up.

This tool can be used for social engineering (choose the BEST answer).

- A) Maltego**
- B) Trout

- C) VisualRoute
- D) Ping Plotter

Explanation: Maltego can be used for social engineering, but is really useful for aggregating data about different social networks, online posts a person does, etc... You don't need hands-on with it to pass the CEH, but definitely one (of many) tools you want to play with, if you decide to be a pentester. The other tools listed are Traceroute tools.

This is known as the "Hacker's Search Engine."

- A) Google
- B) Yahoo
- C) Shodan**
- D) Bing

Explanation: Shodan is correct. The others are search engines (does anyone even use Yahoo search anymore?), but Shodan is used to find vulnerable devices on the Internet.

This TCP header flag is set during the establishment of initial communication. It indicates the negotiation of parameters and sequence numbers.

- A) ACK
- B) SYN**
- C) RST
- D) PSH

Explanation: The ACK (Acknowledgment) flag is set as an acknowledgment to SYN flags. The RST (Reset) flag forces a termination of communications in both directions (think of your kid pulling the power cord on your XBox). The PSH (Push) flag forces the delivery of data without concern for any buffering, so the receiving device does not need to wait for the buffer to fill up before processing the data.

Johnny wants an ordered close to communications. He should use this TCP header flag.

- A) SYN
- B) ACK
- C) RST
- D) FIN**

Explanation: The Finish (FIN) flag signifies an ordered close to communications. The SYN (Synchronize) flag is set during the establishment of initial communication and indicates the negotiation of parameters and sequence numbers. The ACK (Acknowledgment) flag is set as an acknowledgment to SYN flags. The RST (Reset) flag forces a termination of communications in both directions.

When this TCP header flag is set, it indicates the data inside is being sent out of band.

- A) PSH
- B) URG**
- C) SYN
- D) RST

Explanation: The Urgent (URG) flag is correct. The PSH (Push) flag forces the delivery of data without concern for any buffering, so the receiving device does not need to wait for the buffer to fill up before processing the data. The SYN (Synchronize) flag is set during the establishment of initial communication and indicates the negotiation of parameters and sequence numbers. The RST (Reset) flag forces a termination of communications in both directions.

A SYN packet is sent from computer A to computer B, with sequence number 105. A SYN/ACK packet is then sent back to computer A, with the 105 incremented by:

- A) two
- B) three
- C) one**
- D) depends on network latency

Explanation: The SYN/ACK packet sent back by Computer B would be incremented by one (so, 106). It would also contain its own sequence number (let's pretend 221). Computer A then would send back an ACK packet that would contain the sequence number (106) from computer B and an increment of one on its sequence number (so, 222 in this example). You will need to know how much a SYN/ACK response increments by for the exam.

Port 20 and 21.

- A) SMTP
- B) DNS
- C) FTP**
- D) Telnet

Explanation: EC-Council official material doesn't really mention the port numbers too much, but you will need to know the most common ones for the exam. SMTP is port 25. DNS is port 53. Telnet is port 23.

POP3

- A) port 110**
- B) port 25
- C) port 389

D) port 88

Explanation: Port 25 is SMTP. Port 389 is LDAP. Port 88 is Kerberos.

HTTPS

A) port 53

B) port 443

C) port 22

D) port 23

Explanation: Port 53 is DNS. Port 22 is SSH. Port 23 is Telnet.

Kerberos

A) port 23

B) port 21

C) port 88

D) port 3389

Explanation: Port 23 is Telnet. Port 21 is FTP. Port 3389 is RDP.

LDAP

A) port 3389

B) port 389

C) port 443

D) port 53

Explanation: Port 3389 is RDP. Port 443 is HTTPS. Port 53 is DNS.

Tameka wants to open an SSH connection. She should use which port?

A) port 23

B) port 53

C) port 22

D) port 21

Explanation: Port 23 is Telnet. Port 53 is DNS. Port 21 is FTP.

Ports 137-139 include:

A) NetBIOS

B) POP3

C) RDP

D) DNS

Explanation: POP3 is port 110. RDP is port 3389. DNS is port 53.

Port 80

A) HTTPS

B) HTTP

C) DNS

D) LDAP

Explanation: HTTPS is port 443. DNS is port 53. LDAP is port 389.

TFTP

- A) port 110
- B) port 69**
- C) port 25
- D) port 3389

Explanation: Port 110 is POP3. Port 25 is SMTP. Port 3389 RDP.

Snort rule actions include:

- A) Pass, Fumble, Log
- B) Pass, Drop, Alert, Log**
- C) Drop, Track, Log, Alert
- D) Drop, Alert, Log, Track

Explanation: You do need to know this for the CEH exam. Pass, Drop, Alert, and Log are correct. The other answers are made up.

When a system has a port open, it is said to be _____ for a port.

- A) talking
- B) listening**
- C) walking
- D) running

Explanation: The system is said to be listening for a port when it has the port open. The other answers are made up.

A port state of _____ means that the remote side of your connection has closed the connection.

- A) TIME_WAIT
- B) CLOSE_WAIT**
- C) OPEN_WAIT
- D) YELLOW_WAIT

Explanation: The TIME_WAIT state indicates that your side has closed the connection. OPEN and YELLOW_WAIT are made up answers.

Typing this netstat command will display all connections and listening ports.

- A) netstat -an**
- B) netstat -k
- C) netstat -all
- D) netstat -j

Explanation: netstat -an will display all connections and listening ports, with the addresses and port numbers in numerical form. The other answers are made up.

This is an example of a buffer overflow attack.

A) GET /AAAAAAAAAAAAAAAAAAAAA

x90\x90\x90\x83\xec\x27\xeb\x0c\xe7\xe1\xe6\xc1\xc0\xff

A) GET /cgi-bin/cvslog.cgi=<SCRIPT>management.alert</SCRIPT> HTTP/1.1 403

B) GET /scripts/..%255c../windows/system32/cmd.exe?/c+dir HTTP/1.1 200

C) <http://www.madeup.com/script.ext?template=%2e%2e%2f%2e%2e%2f> = passwd

Explanation: A key to recognizing a buffer overflow attack on exams is to look for the x90.

This is an example of XSS (Cross-site Scripting): GET /cgi-

bin/cvslog.cgi=<SCRIPT>management.alert</SCRIPT> HTTP/1.1 403.

This is an example of a Directory Traversal attack: GET

/scripts/..%255c../windows/system32/cmd.exe?/c+dir HTTP/1.1 200.

This is an example of a strange Unicode request:

<http://www.madeup.com/script.ext?template=%2e%2e%2f%2e%2e%2f> = passwd

MAC broadcast:

A) LL:LL:LL:LL:LL:LL

B) FF:FF:FF:FF:FF:FF

C) PP:PP:PP:PP:PP:PP

D) MAC:MAC:MAC:MAC:MAC:MAC

Explanation: The other answers are made up.

Johnny, the world's worst hacker, gets an ICMP Type 3 Code 13 packet. This means:

A) nothing, everything is fine

B) a congestion control message

C) the destination is unreachable because the communication is administratively prohibited (i.e.- traffic is being blocked or filtered by a firewall or router)

D) destination is unreachable and the network is unknown

Explanation: ICMP message Type 4 is a congestion control message. ICMP message Type 3 Code 6 is the destination unreachable and the network is unknown. The "nothing, everything is fine" is a made up answer.

This ICMP message type means Time Exceeded:

A) 4

B) 3

C) 11

D) 0

Explanation: Type 11 is correct. Type 4 is Source Quench. Type 3 is Destination Unreachable. Type 0 is Echo Reply.

This is an answer to a Type 8 Echo Request.

A) **Type 0: Echo Reply**

B) Type 3: Destination Unreachable

C) Type 5: Redirect

D) Type 8: Echo Request

Explanation: Type 0: Echo Reply is an answer to the Type 8: Echo Request. Type 8 is incorrect here for obvious reasons. Type 3: Destination Unreachable is the error message indicating the host or network cannot be reached. Type 5: Redirect is sent when there are two or more gateways available for the sender to use and the best route available to the destination is not the configured default gateway.

A ping message requesting an Echo reply.

A) **Type 8**

B) Type 123

C) Type 3

D) Type 11

Explanation: Type 8 is the Echo Request, which is a ping message that is requesting an Echo reply. Type 3 is Destination Unreachable, which is an error message that indicates the host or network cannot be reached. Type 11 is Time Exceeded, which means the packet took too long to be routed to the destination.

This type of port scan is also known as TCP connect or full open.

A) **Full connect**

B) Stealth

C) XMAS

D) Inverse

Explanation: A Full connect (TCP connect, full open) scan runs through a full connection (the three-way handshake) on all ports. It is easy to detect, but is considered the most reliable. Open ports will respond with a SYN/ACK and closed ports respond with a RST. Know that for the CEH exam. The Stealth scan (half-open or SYN) scan is where only SYN packets are sent to ports, so no completion of the three-way handshake occurs. The XMAS (Christmas) scan is where all of the flags are turned on (so, it's lit up like a Christmas tree). XMAS scans do not work against Windows machines. Know that for your exam. Finally, Inverse scan uses the FIN,

URG, and/or PSH flag to check system ports. If the port is open, there will be no response. If the port is closed, a RST/ACK will be sent as a response. Know that as well for the exam.

This type of port scan does not work on Microsoft Windows.

- A) happy
- B) Inverse
- C) XMAS**
- D) Stealth

Explanation: XMAS scans work on Linux, not Windows. The Inverse scan uses the FIN, URG, and/or PSH flag to check system ports. If the port is open, there will be no response. If the port is closed, a RST/ACK will be sent as a response. It works on Windows. The Stealth scan (half-open or SYN) scan is where only SYN packets are sent to ports, so no completion of the three-way handshake occurs. It also works on Windows. The “happy” answer is made up.

Tasha is a pentester using this nmap command: `nmap 192.168.1.1/24 -sn` What is she doing?

- A) pinging 192.168.1.1
- B) disabling port scanning**
- C) scanning a specific ip
- D) performing a SYN scan

Explanation: The command as `-sn` can be found on the official nmap website under Ref Guide, then Host Discovery. Scanning a specific IP address would be `nmap 192.168.1.1 192.168.2.1`. A SYN scan would be `nmap 192.168.1.1 -sS` A ping of an IP address would be `ping 192.168.1.1`

Keisha wants to enable OS detection, version detection, script scanning, and traceroute.

- A) nmap 192.168.1.1 -A**
- B) `nmap 192.168.1.1 -T5`
- C) `nmap 192.168.1.1 -sA`
- D) `nmap 192.168.1.1 -sU`

Explanation: Nmap commands can be found in-depth on the nmap.org website (I strongly suggest you look through them). The `-T5` is to run an insanely fast scan. `-sA` is a TCP ACK port scan. `-sU` is a UDP port scan.

Johnny, a Hollywood hacker wearing a hoodie and gloves, is trying to do a port scan only.

- A) `nmap 192.168.1.1/24 -sn`
- B) nmap 192.168.1.1-5 -Pn**
- C) `nmap 192.168.1.1`
- D) `nmap 192.168.1.1 -sT`

Explanation: I recommend reviewing the nmap.org website. -sn is to disable port scanning. The nmap 192.168.1.1 answer is just scanning a single IP. -sT is to perform a TCP connect port scan.

Rebecca uses -v in a nmap scan. -v is:

- A) **verbose**
- B) very special
- C) velociraptor
- D) v3 operating system

Explanation: The other answers are made up. I recommend checking out the nmap.org website.

Veena understands that for a nmap scan speed, -T0 to -T5 can be used. -T0 is:

- A) fast scan
- B) super fast scan
- C) **slow scan**
- D) middleground scan

Explanation: T0 is considered the slowest scan speed, with -T5 being the fastest.

The GUI version of NMAP is called:

- A) DOS 3.1
- B) **Zenmap**
- C) Magellan's map
- D) Shodan

Explanation: Zenmap is correct. Shodan is known as the hacker's search engine. The other answers are made up.

hping3 -2 10.0.0.25 -p 80 is:

- A) ICMP ping
- B) ACK scan on port 80
- C) **UDP scan on port 80**

D) SYN scan on port 80

Explanation: UDP is set by using -2 and we also see the -p to designate a port to scan in this case port 80). An ICMP ping would look like: hping3 -1 10.0.0.25 An ACK scan for port 80 would be: hping3 -A 10.0.0.25 -p 80 where the -A is to set the ACK flag. A SYN scan would use -S to set the SYN flag.

Amar wants to perform a SYN scan on ports 50-60. Which hping command should he use?

- A) hping3 -1 50-60 -S 10.0.0.25
- B) hping3 -2 50-60 -S 10.0.0.25
- C) hping3 -8 50-60 -S 10.0.0.25**
- D) hping3 -9 50-60 -S 10.0.0.25

Explanation: The -1 is used to set ICMP mode, the -2 is used to set UDP mode, and the -9 is used to set hping into listen mode, so it triggers on a signature argument (i.e.- hping3 -9 HTTP -l eth0 would look for HTTP signature packets on eth0).

Sara is wanting to fragment a SYN scan, while doing OS fingerprinting. She could use:

- A) nmap -sS -A -f 172.17.15.12**
- B) nmap -sS -A 172.17.15.12
- C) nmap -sA 172.17.15.12
- D) nmap -sX 172.17.15.12

Explanation: The -f gives this one away. The -sA is for an ACK scan. The -sX is for the Xmas scan. The other answer does not include fragmentation and is only performing a SYN scan, while doing OS fingerprinting.

A hacker is spoofing an IP address during a TCP scan. This means:

- A) data is in limbo
- B) data coming back to the spoofed IP address will not make it to the hacker**
- C) data is being sent in a CCP
- D) data is in Xmas format

Explanation: Since the IP address is spoofed, the hacker will not see any responses from the other system. The other answers are made up.

In its simplest form, this system is an intermediary between you and your targets.

- A) honeypot
- B) proxy**
- C) Google search

D) Nessus

Explanation: A honeypot is used to draw in attackers and see what/how they are attacking. Nessus is a vulnerability scanner. Google search is used for searching.

This is a live operating system that can be run from a USB and is intended to anonymize the source.

A) Windows

B) Linux

C) Tails

D) Mac OS

Explanation: Tails is correct. Windows is probably the least anonymous of the others listed.

TOR stands for:

A) This Operating Randomly

B) The Onion Router

C) Taser Onion Routing

D) The Onion Route

Explanation: TOR is The Onion Router. The other answers are made up.

Vulnerability scanners include all of the following EXCEPT:

A) Nessus

B) Qualys FreeScan

C) CyberGhost

D) OpenVAS

Explanation: CyberGhost is a VPN. All others are vulnerability scanners, with Nessus being the most used.

In Windows, the security identifier (SID) is what number in this:

S-1-5-21-3874928736-367528774-1298337465-500

A) 367528774

B) 500

C) 1298337465

D) 21

Explanation: 500 is correct and is the administrator account. The other numbers are just a part of the random SID string.

A SID of 1014 would tell us:

- A) it is the administrator account
- B) it is the guest account
- C) it is the 14th user account on the system**
- D) it is the 1014th user account on the system

Explanation: All users created for the system start at 1000, so 1014 would be for the 14th user account on the system. The SID of 500 is the administrator account and a RID (resource identifier) of 501 is for the guest account.

Priyanka uses this: telnet 192.168.1.15 80

What is she doing?

- A) mapping telnet to port 80
- B) banner grabbing**
- C) hacking the NSA
- D) opening TOR

Explanation: Banner grabbing is correct. Port 80 is for HTTP, but here she is using the telnet command in the hope to get an error message back, with additional information about the OS in use.

The White Hat hacker is using what tool for banner grabbing here?

nc 192.168.1.20 80

- A) netcat**
- B) telnet
- C) Nessus
- D) Ecora Auditor

Explanation: Ecora Auditor (as the name implies) is used for auditing. Nessus is a vulnerability scanner.

All of the following can be used for Linux enumeration EXCEPT:

- A) finger
- B) showmount

- C) rpcinfo
- D) tracert**

Explanation: tracert is used in Windows to trace the path to the destination and uses ICMP Echo requests. All other answers can be used to enumerate Linux.

This command should be piped to netcat and sends continuous text to netcat, until either host terminates the session by sending a break signal or by killing the terminal process.

- A) piper
- B) plumb
- C) yes**
- D) no

Explanation: The yes command should be piped to netcat and sends continuous text to netcat, until either host terminates the session by sending a break signal or by killing the terminal process.. The other answers are made up.

All of the following can be used for NetBIOS enumeration EXCEPT:

- A) nbtstat
- B) Hyena
- C) SuperScan
- D) BigMac**

Explanation: BigMac is a made up answer. The others can all be used to enumerate NetBIOS.

This sets the time across your network.

- A) Hyena
- B) NTP**
- C) JXR
- D) BP

Explanation: NTP (Network Time Protocol) sets the time across your network. Hyena can be used for NetBIOS enumeration. JXR and BP are made up answers.

In SMTP, the VRFY command.

- A) validates the user**
- B) verifies the NetBIOS
- C) verifies the IP address has not changed before the scheduled time
- D) defines recipients

Explanation: The RCPT TO defines recipients. The other two answers are made up.

This SMTP command provides the actual delivery addresses of mailing lists and aliases.

- A) VRFY
- B) EXPN**
- C) RCPT TO
- D) telnet

Explanation: The EXPN command provides the actual delivery addresses of mailing lists and aliases. The RCPT TO command defines recipients. The VRFY command validates the user. Telnet is not a SMTP command.

SNMP uses this as a form of password.

- A) community string**
- B) roger string
- C) passive string
- D) active string

Explanation: SNMP uses a community string as a form of password. The read-only version of the community string allows a requester to read virtually anything SNMP can get from the device. The read-write version is used to control access for the SNMP SET requests. The roger string, passive string, and active string are all made up answers.

Sniffing is also called this by law enforcement.

- A) sniffadoodle
- B) wiretapping**
- C) pentesting
- D) VRFY

Explanation: Sniffing is also called wiretapping. Sniffing is a component of pentesting, but the terms are not synonyms. The SMTP VRFY command validates the user.

An IPv4 local loopback address.

- A) 192.168.55.297
- B) 192.168.2.64
- C) 127.0.0.1**

D) 157.0.0.6

Explanation: 127.0.0.1 is correct. All of the other answers are made up.

The MAC address is also known as the _____ address.

- A) random
- B) physical**
- C) logical
- D) phantom

Explanation: The MAC is the physical address. It is burned onto a NIC card. The other answers are made up.

This ARP command will display the current ARP cache.

- A) arp -xyz
- B) arp -a**
- C) arp -b
- D) arp -z

Explanation: arp -a will display the current ARP cache. The other answers are made up.

This is the process of maliciously changing the ARP cache on a machine to inject faulty entries.

- A) ARP poisoning**
- B) ARP listening
- C) ARP attack
- D) DHCP starvation

Explanation: ARP poisoning is correct. The other ARP answers are made up. DHCP starvation is where attackers try to exhaust all available addresses from the server.

All of the following are used to filter Wireshark packets, EXCEPT:

- A) ==
- B) or
- C) yes**
- D) &&

Explanation: The yes choice is a made up answer and is incorrect. The Equal to (==) means the packet will display if the argument appears in the packet, the And (&&) means the packet will display only if both arguments appear in the packet, and the Or (or) means the packet will display if either argument appears in the packet.

All of the following are packet sniffing tools, EXCEPT:

- A) Wireshark
- B) Recuva**
- C) tcpdump
- D) Capsa Network Analyzer

Explanation: Recuva is a digital forensics tool for recovering files. The other choices can all be used for packet sniffing.

This type of IDS (Intrusion Detection System) compares packets against a list of known traffic patterns that indicate an attack.

- A) anomaly-based
- B) signature-based**
- C) forensic-based
- D) Wireshark-based

Explanation: A signature-based IDS compares packets against a list of known traffic patterns that indicate an attack. An anomaly-based IDS learns the “normal” behavior of the network and alerts on anything outside of that behavior. One downside is if the network was already compromised before the anomaly-based IDS was added. Forensic-based and Wireshark-based are both made up answers.

A hacker can try to bypass an IDS with this:

- A) TCP packets
- B) fragmentation**
- C) IPv6 packets
- D) wiretapping

Explanation: Fragmentation is where the attacker sends fragmented packets that will be reassembled after going past the IDS. The other answer choices are made up.

When an IDS reports traffic as being fine, but it is not.

- A) false positive
- B) false negative**
- C) positive positive
- D) true positive

Explanation: A false positive is when the IDS alerts that an intrusion has occurred, when in fact the network is fine. The other two answer choices are made up.

This type of IDS normally resides on the host itself.

- A) NIDS
- B) HIDS**
- C) LIDS

D) RIDS

Explanation: HIDS (host-based intrusion detection system) is correct. NIDS is network-based intrusion detection system. LIDS and RIDS are made up answers.

tcp.flags == 0x16

A) looks for SYN packets

B) looks for ACK packets

C) looks for RST packets

D) looks for URG packets

Explanation: This command is looking for ACK packets. In Wireshark filtering, the assigned decimal numbers for packets are: FIN=1 SYN=2 RST=4 PSH=8 ACK=16 URG=32 In this example, we were looking at the number 16, which tells us it is ACK packets. For example, if we had tcp.flags==0x18 it would tell us that we are looking for both SYN (2) and ACK (16) packets.

This Snort file resides in /etc/snort on Linux computers and c:\snort\etc\ on Windows.

A) log file

B) configuration file

C) user file

D) etc file

Explanation: The Snort configuration file resides in /etc/snort on Linux computers and c:\snort\etc\ on Windows. The other answer choices are made up.

_____ means if there is not a firewall rule defined to allow a packet to pass, the packet is blocked.

A) implicit deny

B) implicit approve

C) explicit allowed

D) always allowed

Explanation: Implicit deny is correct. An administrator can explicitly allow certain packets to pass the firewall. The other two answers are made up. A key point to remember for the exam is an implicit deny rule should always be the last rule. For example, if the firewall checks its ruleset and sees the implicit deny, it will block all remaining traffic, even if you have a hundred other rules in place.

NAT is:

- A) network address translation**
- B) new address translation
- C) network add-on transport
- D) new add-on transport

Explanation: NAT stands for network address translation. The other answers are made up.

PAT is:

- A) pacific address time
- B) port address translation**
- C) patterned address transport
- D) protocol and transport

Explanation: PAT stands for port address translation. Like, NAT (network address translation) it is used to allow an internal address to use an external address. With PAT; however, many internal addresses can use a single external address.

This sits between the internal and external network and is designed to help protect the internal network resources from attack.

- A) bastion host**
- B) Snort
- C) Wireshark
- D) tcpdump

Explanation: Snort is an IDS. Wireshark and tcpdump can be used for packet sniffing.

Layer 6 of the OSI model.

- A) Session
- B) Physical
- C) Datalink
- D) Presentation**

Explanation: The seven layers of the OSI model are: Layer 1-Physical Layer 2-Datalink Layer 3-Network Layer 4-Transport Layer 5-Session Layer 6-Presentation Layer 7-Application

This type of firewall looks at the headers of packets coming through a port and decide whether to allow them, based on the access control lists (ACLs) that are configured.

- A) stateful inspection
- B) packet-filtering**

- C) circuit-level gateway
- D) application-level

Explanation: A packet-filtering firewall looks at the headers of packets coming through a port and decide whether to allow them, based on the access control lists (ACLs) that are configured. A stateful inspection firewall allows for tracking of the status of the connection. For example, if a packet arrives with an ACK flag set, but there is no record of the original SYN packet being sent, it would be considered malicious traffic. The circuit-level gateway firewall works at the Session layer (OSI model layer 5) and allows or prevents data streams (it is not necessarily concerned with individual packets). The application-level firewall filters traffic like a proxy in that it allows specific applications (services) in and out of the network based on its rule set.

A hacker wants to bypass a firewall with HTTPS tunneling. He knows this port is used.

- A) 23
- B) 25
- C) 443**
- D) 80

Explanation: Port 443 is for HTTPS. Port 23 is telnet. Port 25 is SMTP. Port 80 is for HTTP.

This is the process of walking through every port against a firewall to determine what is open.

- A) firewalking**
- B) pathing
- C) firepathing
- D) firewallrunning

Explanation: Firewalking is the process of walking through every port against a firewall to determine what is open. The other answers are made up.

This is a system set up as a decoy to entice attackers.

- A) honeypot**
- B) packet-filtering firewall
- C) application-level firewall
- D) honeyjar

Explanation: A honeypot is a system set up as a decoy to entice attackers. A packet-filtering firewall looks at the headers of packets coming through a port and decide whether to allow them, based on the access control lists (ACLs) that are configured. The application-level firewall

filters traffic like a proxy in that it allows specific applications (services) in and out of the network based on its rule set. Honeyjar is a made up answer.

Ronnie, a security engineer, knows that this is located at C:\windows\system32\config

- A) MAS file
- B) SAM file**
- C) MSA file
- D) LAM file

Explanation: The SAM (Security Accounts Manager) file stores user authentication credentials (like hashed passwords).

They maintain WebGoat.

- A) NIST
- B) EC-Council
- C) OWASP**
- D) Apache

Explanation: The Open Web Application Security Project (OWASP) maintains WebGoat and also maintains top ten lists for Web security. NIST is a standards framework. EC-Council is a certification vendor for exams, like the CEH and CHFI. Apache is used as a web server.

In _____ hashing, a password of seven characters or less will result in the hash value AAD3B435B51404EE for the last seven, blank characters.

- A) AM
- B) LM**
- C) OM
- D) RM

Explanation: LM hashing is correct. The other answers are made up.

SELECT * FROM users WHERE name = " OR '1' = '1' ;

- A) UNION SQL Injection attack
- B) Tautology-based SQL injection attack**
- C) Blind SQL Injection
- D) Error-based SQL injection

Explanation: This is an example of a Tautology-based SQL injection attack. In this attack, a "true" clause is used to bypass user authentication. In a UNION attack, the attacker uses a

UNION clause to append a malicious query to the requested query. A Blind SQL injection attack occurs when the attacker knows that the database is susceptible to injection, but the error messages and screen returns don't come back to the attacker. In Error-based SQL injection, the focus is to enter poorly constructed statements in an effort to get the database to respond with table names and other information in the returned error messages.

This is the most secure type of wireless listed.

- A) WPA
- B) WPA2**
- C) WEP
- D) WEP-1

Explanation: WEP is the weakest form of security listed. WEP-1 is made up. WPA uses TKIP (temporal key integrity protocol) , which uses a message integrity check (MIC).

This can be used to extract WEP encryption keys.

- A) aircrack-ng**
- B) Recuva
- C) jv16
- D) Snort

Explanation: aircrack-ng is correct. Recuva is for file recovery. jv16 is used in malware analysis to check for installation file changes. Snort is an IDS.

Jailbreaking tool for Android.

- A) Pangu
- B) Redsn0w
- C) SuperOneClick**
- D) GeekSn0w

Explanation: SuperOneClick is used to jailbreak Android. The other tools are all used for iOS.

Kismet is used for:

- A) website hacking
- B) SQL injection attacks
- C) wireless sniffing**
- D) URL hacking

Explanation: Kismet is an 802.11 Layer 2 wireless sniffer.

CSRF is also known as:

- A) **session riding**
- B) XSS attack
- C) watering hole attack
- D) SQL injection attack

Explanation: Cross-Site Request Forgery (CSRF) is also known as session riding or a one-click attack. This attack exploits a victim's active session with a trusted site.

This is designed to exchange structured information in web services and uses XML to format information. It allows applications running on one platform to communicate with applications running on a different platform.

- A) SQL
- B) XSS
- C) **SOAP**
- D) CSRF

Explanation: SOAP (Simple Object Access Protocol) is designed to exchange structured information in web services and uses XML to format information. It allows applications running on one platform to communicate with applications running on a different platform. SQL, XSS, and CSRF are all types of Web attacks.

All of the following are wireless standards, EXCEPT:

- A) 802.11a
- B) 802.11n
- C) 802.11g
- D) **802.57x**

Explanation: 802.57x is a made up answer. All of the other answers are wireless standards. 802.11b (not listed) is also a wireless standard.

This is a simple denial of service against the bluetooth device.

- A) Bluebugging
- B) Bluesnarfing
- C) **Bluesmacking**
- D) Bluejacking

Explanation: Bluesmacking is a simple denial of service, similar to a ping of death attack. Bluebugging is remotely taking control of a bluetooth device. Bluesnarfing is the actual theft of

data from a mobile device. Bluejacking consists of sending unsolicited messages to and from mobile devices.

All of the following are Bluetooth tools, EXCEPT:

- A) BT Browser
- B) Blooover
- C) BH Bluejack
- D) PhoneSnoop**

Explanation: PhoneSnoop is a tool (spyware that is a component of the Bugs toolkit) for BlackBerry devices. It allows you to remotely activate the microphone of the device and listen.

Phishing fraud where the attacker utilizes SMS to send messages to the victim that contain a malicious link or telephone number.

- A) Zishing
- B) SMiShing**
- C) ZitMo
- D) Lishing

Explanation: SMiShing is correct. ZitMo (Zeus in the Middle) is a type of malware for Android phones. The other two answers (Lishing and Zishing) are made up.

The provider offers on-demand applications to subscribers over the Internet.

- A) SaaS**
- B) PaaS
- C) IaaS
- D) LaaS

Explanation: Software as a Service (SaaS) offers on-demand applications to subscribers over the Internet. PaaS (Platform as a Service) provides a development platform that allows the subscriber to develop applications, without building out the infrastructure themselves that it would normally take to develop the applications. Infrastructure as a Service (IaaS) is virtualized computing resources over the Internet and allows organizations to scale up or down, depending on needs. LaaS is a made up answer.

This is shared by several organizations, usually with the same policy and compliance considerations.

- A) private cloud
- B) public cloud
- C) community cloud**
- D) platform cloud

Explanation: Community clouds are shared by several organizations, usually with the same policy and compliance considerations. A private cloud is operated for a single organization (single tenant environment). A public cloud is a model where services are provided over the Internet for public use. Platform cloud is a made up answer.

This is a leading professional organization that is devoted to promoting cloud security best practices and organizing cloud security professionals.

- A) CIA
- B) CSA**
- C) NSA
- D) FBI

Explanation: CSA (Cloud Security Alliance) is a leading professional organization that is devoted to promoting cloud security best practices and organizing cloud security professionals. The other choices are agencies of the United States government and are not industry professional organizations (CIA = Central Intelligence Agency, NSA = National Security Agency, FBI = Federal Bureau of Investigation).

In this type of attack, a SOAP message is intercepted and the data in the envelope is changed and then replayed.

- A) Session riding
- B) side channel
- C) wrapping**
- D) CSRF

Explanation: In a wrapping attack, a SOAP message is intercepted and the data in the envelope is changed and then replayed. Session riding and CSRF (Cross-Site Request Forgery) are similar. A side channel (aka- cross-guest VM breach) attack is where an attacker gains control of an existing VM on the same physical host as the target.

These are programs that allow you to bind the executable of your choice (say a Trojan) to an innocent file that your target will not mind opening.

- A) crypters
- B) wrappers**

- C) packers
- D) lovers

Explanation: Wrappers are programs that allow you to bind the executable of your choice (say a Trojan) to an innocent file that your target will not mind opening. A crypter is a tool that uses a combination of encryption and code manipulation to render malware undetectable to antivirus and other security monitoring products. Packers use compression to pack the malware executable into a smaller size, which is intended to make the malware harder to detect for some antivirus programs. Lovers might be nice, but it is a made up answer in the context of security.

These are tools that use a combination of encryption and code manipulation to render malware undetectable to antivirus and other security monitoring products.

- A) crypter**
- B) packer
- C) wrapper
- D) exploit kit

Explanation: A crypter is a tool that uses a combination of encryption and code manipulation to render malware undetectable to antivirus and other security monitoring products. A packer uses compression to pack the malware executable into a smaller size, which is intended to make the malware harder to detect for some antivirus programs. A wrapper is a program that allows you to bind the executable of your choice (say a Trojan) to an innocent file that your target will not mind opening. An exploit kit is a platform from which you can deliver payloads and exploits (i.e.- Blackhole, Bleeding Life, etc...).

This is software that appears to perform a desirable function for the user running it, but instead it performs a function, usually without the user's knowledge, that steals information or harms system data.

- A) packer
- B) Trojan**
- C) wrapper
- D) crypter

Explanation: A packer uses compression to pack the malware executable into a smaller size, which is intended to make the malware harder to detect for some antivirus programs. A wrapper is a program that allows you to bind the executable of your choice (say a Trojan) to an innocent file that your target will not mind opening. A crypter is a tool that uses a combination of encryption and code manipulation to render malware undetectable to antivirus and other security monitoring products.

This is the encrypted version of Netcat.

- A) EncryptedCat
- B) LyptCat

C) CryptCat

D) EncptCat

Explanation: CryptCat is correct. The other answer choices are made up.

This is a self-replicating program that reproduces its code by attaching copies into other executable codes (it produces a copy of itself by attaching itself to another program or document).

A) worm

B) crypter

C) crypto

D) virus

Explanation: A worm replicates, executes, and spreads itself across network connections. A crypter is a tool that uses a combination of encryption and code manipulation to render malware undetectable to antivirus and other security monitoring products. Crypto is a made up answer.

Johnny downloaded a file from a torrent and now is locked out of his system, with a message that he must pay 2 Bitcoin to get access to his files.

A) Boot sector virus

B) ransomware

C) Shell virus

D) Polymorphic code virus

Explanation: Ransomware is malware that locks you out of your own system resources and demands an online payment of some sort. A Boot sector virus (aka a system virus) moves the boot sector to another location on the hard drive, forcing the virus code to be executed first, which makes this type of virus nearly impossible to get rid of. A Shell virus works similar to a Boot sector virus in that it wraps itself around an application's code and causes the virus code to be run before the application's code. A Polymorphic code virus mutates its code, using a built-in polymorphic engine, and is difficult to detect and remove because its signature constantly changes.

This type of virus modifies directory table entries, so that the user or system processes are pointed to the virus code itself, instead of the intended application. It does not change the files themselves or plant additional files. It is only changing the pointers for the directory.

A) Boot sector virus

B) Cluster virus

C) Shell virus

D) ransomware

Explanation: Cluster virus is correct. A Boot sector virus (aka a system virus) moves the boot sector to another location on the hard drive, forcing the virus code to be executed first, which makes this type of virus nearly impossible to get rid of. A Shell virus works similar to a Boot sector virus in that it wraps itself around an application's code and causes the virus code to be run before the application's code. Ransomware is malware that locks you out of your own system resources and demands an online payment of some sort.

Sara is scared of a virus that is designed to infect Microsoft Office products, like Word and Excel.

- A) **Macro virus**
- B) Polymorphic code virus
- C) Shell virus
- D) Stealth virus

Explanation: A Macro virus is usually written in Visual Basic and infects template files created by Word and Excel (most newer versions of these automatically disable Macros). An example is the Melissa virus. A Polymorphic code virus mutates its code, using a built-in polymorphic engine, and is difficult to detect and remove because its signature constantly changes. A Shell virus works similar to a Boot sector virus in that it wraps itself around an application's code and causes the virus code to be run before the application's code. A stealth virus (aka tunneling virus) attempts to evade antivirus by intercepting the antivirus' request to the operating system and returning them to itself, instead of the OS. The virus then alters the requests and sends them back to the antivirus as uninfected, which makes the virus appear to be clean.

This was a denial of service worm that attacked buffer overflow weaknesses in Microsoft SQL services that could fit inside a single packet.

- A) Code Red
- B) Darloz
- C) **Slammer**
- D) Nimda

Explanation: Slammer is also known as SQL Slammer and is only briefly mentioned in the ECC material. Code Red is a worm that exploits Microsoft IIS servers and was seen back in 2001. Darloz is known as the worm for the Internet of Things. It is a Linux-based worm that targets things like security cameras and routers. Nimda was a worm that spread through e-mail, network shares, and websites. It also took advantage of backdoors left behind by the Code Red worm.

This is a system that is set up to check physical media, device drivers, and other files for malware before introducing them to the network.

- A) Cowdip
- B) Sheepdip**
- C) Goatdip
- D) Elephantdip

Explanation: Sheepdip is a system that is set up to check physical media, device drivers, and other files for malware before introducing them to the network. This is normally a computer that is isolated from the network and only used for this purpose. The other answer choices are made up.

This is the preferred communications channel to signal a bot.

- A) IRC**
- B) LOC
- C) LRC
- D) WRC

Explanation: IRC (Internet Relay Chat) is the preferred communications channel to signal a bot. The other answers are made up. For the exam, just know what IRC stands for.

This type of attack consumes all available bandwidth for a system or service.

- A) SYN flood
- B) Volumetric**
- C) Fragmentation
- D) TCP state-exhaustion

Explanation: A Volumetric (or bandwidth) attack consumes all available bandwidth for a system or service. A SYN flood is where thousands of SYN packets are sent to the target, but no response is ever given to the SYN/ACK packets sent by the target system. The target must wait a certain amount of time to receive an answer to the SYN/ACK packets it had sent, so this then causes the system to become bogged down. A fragmentation attack takes advantage of the system's inability to reconstruct fragmented packets. A TCP state-exhaustion attack attempts to consume the connection state tables of load balancers, firewalls, and application servers.

This type of attack sends a large number of pings to the broadcast address of the subnet, with the IP address spoofed to that of the intended target. This then causes all devices on the subnet to begin sending a ping response to the target system, exhausting all of its resources.

- A) teardrop
- B) smurf**
- C) LAND
- D) LOIC

Explanation: A smurf attack is correct. A teardrop attack is where a large number of garbled IP fragments, with overlapping and oversized payloads, are sent to the target system. A LAND

attack sends a SYN packet to the target system, with the IP address spoofed to that of the target. This can cause the target system to loop endlessly and crash. The LOIC (Low Orbit Ion Cannon) is used to flood targets with TCP, UDP, and HTTP requests.

In this IPsec mode, the payload and ESP trailer are encrypted; however, the header of the original packet is not.

A) transport mode

B) tunnel mode

C) VPN mode

D) NAT mode

Explanation: IPsec is also mentioned throughout the ECC text. In transport mode, the header of the original packet is not encrypted. In tunnel mode, the original packet is encapsulated in the new IPsec shell, so everything is encrypted. Know the difference between these for the CEH exam. VPN mode and NAT (network address translation) mode are made up answers.

In a XOR operation, a 1 (one) means the values are:

A) the same

B) different

C) bittable

D) ESP

Explanation: For a XOR operation, different values will be a 1 (one) and the same values will be a 0 (zero). Memorize that for your exam. ESP (Encapsulating Security Payload) is a protocol that provides origin authenticity and integrity. Bittable is a made up answer.

This type of encryption uses a single key or shared key. Basically, one key is used to encrypt and decrypt the data.

A) asymmetric

B) Ettercap

C) symmetric

D) ADS spy

Explanation: Symmetric encryption uses a single or shared key to encrypt and decrypt the data. It is faster than asymmetric encryption. This type of encryption provides confidentiality, but not nonrepudiation. Asymmetric encryption is a key pair system. One key is used to encrypt the data and another key is used to decrypt (public and private key). The private key is kept secured on the system and the public key (the encrypting key) is what is sent to the receiver. Ettercap is a sniffer and tool that can be used for attacks, like man-in-the-middle. ADS spy helps you locate alternate data streams.

This is a stream cipher and not a block cipher.

- A) Blowfish
- B) RC5
- C) RC4**
- D) Twofish

Explanation: RC4 is a variable key-size symmetric-keystream cipher. RC5 is a symmetric-key block cipher. Blowfish and Twofish are also block ciphers, but not really mentioned in the ECC material.

This is a block cipher that is used in PGP (Pretty Good Privacy) for bulk message encryption.

- A) RC4
- B) IDEA**
- C) RSA
- D) RC5

Explanation: IDEA (International Data Encryption Algorithm) is a block cipher that is used in PGP (Pretty Good Privacy) for bulk message encryption. It uses a 128 bit key and was designed to replace DES. RSA is also used in PGP; however, it is used for key transport. RC4 is a variable key-size symmetric-keystream cipher. RC5 is a symmetric-key block cipher.

Message Digest functions (hashing algorithms) are:

- A) two way mathematical functions
- B) one way mathematical functions**
- C) four way mathematical functions
- D) three way mathematical functions

Explanation: Hashing algorithms (seen in the ECC material as Message Digest Functions) are one way mathematical functions that take an input and produce a fixed length string (hash), based on the data bits in the input. For the exam, just know that hash is going to be a one-way function. The other answers are made up.

SHA-1 has:

- A) 128 bit hash
- B) 160 bit hash**

- C) 256 bit hash
- D) 2048 bit hash

Explanation: SHA-1 has a 160 bit hash value output. The other answers are made up.

Tony wants to use a technique that makes cracking passwords more difficult.

- A) salting**
- B) peppering
- C) GAK
- D) CA

Explanation: Salting is the process of using random bits to generate different hashes of the same password. Peppering is a made up answer. GAK (government access to keys) is also referred to as key escrow and is where companies provide their encryption keys to the government, and the government promises to only use them when they really need to. CA (Certificate Authority) acts as a third party to the organization. Its job is to create and issue digital certificates that can then be used to verify identity. It also tracks certificates with a certificate management system and maintains a certificate revocation list to see which certificates have problems or which have been revoked.

An attacker wears a fake badge and attempts to gain access to a secure area by closely following an authorized person through the door. It implies this access is gained without the authorized user's consent.

- A) piggybacking
- B) rubbernecking
- C) tailgating**
- D) POODLE

Explanation: Tailgating is correct. Piggybacking is where the attacker will request for an authorized person to open the door, citing things like they had forgotten their badge at home. The main difference between tailgating and piggybacking you will probably see asked pertains to the attacker wearing a fake badge to gain access and if the authorized user actually knows what is occurring (consent). POODLE is an attack that interrupts all handshake attempts by TLS and forces the browser to degrade back to using SSL. Rubbernecking is a made up answer.

This is a spouse, friend, or event client of an employee that uses the employee's credentials to gain access, even if this is without the consent of the employee.

- A) pure insider
- B) insider associate
- C) insider affiliate**
- D) outside affiliate

Explanation: Insider affiliate is correct. A pure insider is the employee (aka- insider threat). The insider associate is someone with limited, but authorized access. This could be people like guards or the cleaning crew. The outside affiliate is a non-trusted outsider who uses open access to gain access to the company's resources. So, for example, this could be someone gaining unauthorized access to wireless access points.

Challenges of IoT devices include all the following, EXCEPT:

- A) security concerns
- B) longevity and compatibility concerns
- C) lack of standards
- D) none of the above**

Explanation: Security concerns, longevity and compatibility concerns, a lack of standards for IoT devices, connectivity issues, and intelligent analysis and actions are all challenges of IoT devices.

The OWASP Top Ten for IoT vulnerabilities includes all the following, EXCEPT:

- A) Insecure Web interface
- B) Privacy concerns
- C) Insecure cloud interface
- D) Secure software development**

Explanation: Having secure software development principles used in IoT design is not a vulnerability listed on the OWASP Top Ten list.

The Common Vulnerability Scoring System (CVSS) consists of three metrics, which include all the following EXCEPT:

- A) Base Metrics
- B) PW Metrics**
- C) Temporal Metrics
- D) Environment Metrics

Explanation: PW Metrics is a made up answer. Base Metrics represents the inherent qualities to a vulnerability. Temporal Metrics represents the features that keep changing during the lifetime of a vulnerability. Environmental Metrics represent the vulnerabilities that are based on a particular environment or implementation.

This is one of the most common vulnerability scanners in use.

- A) Snort
- B) Edge
- C) Nessus**
- D) Firefox

Explanation : Firefox and Edge are both Web browsers. Snort is an IDS (Intrusion Detection System). Nessus is the correct answer and the Nessus Professional version is what is used. Tenable is the organization behind the Nessus scanner.